WHAT IS CLAIMED IS:

1. A method of defining the security condition of a computer system, comprising:

specifying an identity of an attack;

specifying at least one attribute of the specified attack;

specifying at least one policy definition with respect to the specified attack; and

specifying at least one attribute of the specified policy definition.

2. The method, as set forth in claim 1, further comprising:

specifying a computing platform of the computer system; and

specifying a data signature of the specified attack on the computing platform.

3. The method, as set forth in claim 1, further comprising:

specifying a security category of the specified attack; and

specifying at least one policy group with respect to the specified security category.

4. The method, as set forth in claim 1, further comprising specifying a security product executing on the computer system.

5. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the specified attack.

6. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack.

7. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important.

8. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack.

9. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an application operable to respond to a breach of the computer system by the specified attack.

10. The method, as set forth in claim 1, wherein specifying a signature of the specified attack comprises:

specifying a network protocol;

specifying a data pattern; and

specifying an action in response to detecting the specified network protocol and data pattern.

11. The method, as set forth in claim 1, wherein specifying a signature of the specified attack comprises specifying a direction of data flow.

12. A method of defining vulnerability conditions of a system coupled to a global network, comprising:

specifying a name of an attack associated with a vulnerability of the system;

specifying at least one attribute of the specified attack, and the severity of the specified attack associated with a breach of the computer system by the specified attack;

specifying a policy definition with respect to the specified attack;

specifying at least one attribute of the specified policy definition;

specifying a computing platform of the system.

13. The method, as set forth in claim 12, further comprising:

specifying a security category of the specified attack; and

specifying at least one policy group with respect to the specified security category.

14. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack.

15. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying an application operable to respond to a breach of the computer system by the specified attack.

16. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying a source of an application operable to repair the vulnerability.

17. A system of defining security conditions of a computer system, comprising:

a vulnerability description file containing a definition of at least one attack and a definition of at least one policy item for the attack;

an interpreter operable to parse the at least one attack and at least one policy item definition in the vulnerability description file and organize the parsed definitions pursuant to a predetermined format; and

a data storage operable to store the parsed and organized at least one attack and at least one policy item definition, wherein the data storage is accessible by at least one security application.

18. The system, as set forth in claim 17, wherein the data storage is a relational database having a plurality of tables.

19. The system, as set forth in claim 17, wherein the data storage is a memory.

20. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of a security product.

21. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of a security category providing a grouping of the at least one attack, and a definition of a policy group providing a grouping of the at least one policy item.

22. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of a computing platform.

23. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of at least one attribute of the at least one attack.

24. The system, as set forth in claim 17, wherein the vulnerability description file further comprises an identification of the severity associated with a breach of the computer system by the at least one attack.

25. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a description of the at least one attack.

26. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of how information are to be displayed and reported to the user in response to generated results with respect to the at least one attack.

27. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a definition of an application operable to respond to a breach of the computer system by the at least one attack.

28. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a signature of the specified attack having:

a network protocol;

a data pattern; and

an action in response to detecting the specified network protocol and data pattern.

29. The system, as set forth in claim 17, wherein the vulnerability description file further comprises a signature of the specified attack having a direction of data flow.